REMARKS

The Examiner is thanked for the comments in the Action and for, with supervising Examiner G. Barrón, granting us a telephone interview on 03/07/2003. This has helped us considerably in understanding the rationale for the outstanding rejections and in drafting this Response thereto.

It is our understanding that claims 1-20 remain pending in this application.

Preliminary item:

Please note that our docket number for this matter has changed, from INFOP002 to 60468.300201. Entry of the new number into the Office's databases would be appreciated.

We proceed now with reference specifically to the numbered items in the Action.

Items 1-2 and 4-5:

These appear informational in nature and are understood to require no reply.

Item 3 (§103(a) rejections):

Claims 1-20 are rejected as being obvious over McArdle et al. in view of Hussey. Respectfully, we urge that this is moot in view of the present amendments to the claims. No new subject matter is added by the amendments.

Claim 1 now specifically recites that the sender provides an id and password, and receives a message key from the security server. Similarly, claim 11 now specifically recites that the receiver provides an id and password, and receives the message key from the security server. Claim 20 already had effectively similar language. These amendments make explicit aspects of the present invention that McArdle and Hussey do not teach or reasonably suggest, and that Examiners Zand and Barrón stressed in the interview of 03/07/2003. Support for these amendments can be seen in FIG. 1, so no new subject matter is added by them.

Claims 1 and 20 now also specifically recite that a secure e-mail is not communicated via the security server. Claim 11 deals with secure e-mails after they are received by a receiver, so how they are communicated prior to that is not relevant. These amendments make explicit an additional aspect of the present invention that McArdle and Hussey do not teach or reasonably suggest, and that Examiners Zand and Barrón also stressed in the interview of 03/07/2003.

Support for these amendments can be also seen in FIG. 1, so no new subject matter is added by them either.

In view of the above, we respectfully urge that the present claimed invention is clearly distinguishable from McArdle and Hussey and we urge that the §103(a) rejections be withdrawn and all of the claims allowed.

In the alternative, we include the following additional remarks, which essentially restate the rationale in our draft response discussed in the interview of 03/07/2003 for why the claimed invention is distinguishable from McArdle and Hussey.

As a key point, we note that both McArdle and Hussey teach systems that "see" the e-mails and examine their content. In the case of McArdle, the system acts as a proxy that intercepts an e-mail to determine if it should be forwarded to recipients (see e.g., Abstract "*the Agent intercepts e-mail normally bound for the mail server* ..."). Accordingly, the e-mail is not a single "secure e-mail" all of the way between the sender and the recipient here. In the case of Hussey, the system is an actual recipient of the e-mail (see e.g., Abstract "[t]*he system include a plurality of clients disposed for communication with a database server* ..."). In contrast, the claimed invention does not send its secure e-mail 14 via its security server 24 (its "key server")(see e.g., FIG. 1). As depicted by the solid lines in FIG. 1 for stages 38 and 40, the secure e-mail 14 is sent via the EMail Server 22 (typically an entirely conventional e-mail server), and it remains secure all of the way from the sender to the recipient. This is a key distinction of the claimed invention over the prior art, such as McArdle and Hussey, and provides the clear advantage that a security server, acting alone, can never breach the security of the secure e-mail.

Turning now specifically to the text of item 3, the Action here states "*wherein the message id, message keys are stored in a server to be received by sender and the receiver (see fig.3, item 380; col.3, lines 26-67 and col.4, lines 1-27 and col.2, lines 44-46)* ...." However, item 380 is "*back-end server software 380 running on a server computer*" (col. 9, in. 62-63) and what has been missed here is that this is a different server than Applicant's security server. Applicant's security server stores keys but never needs to receive the secure e-mail. In contrast, McArdle "*works in conjunction with a standard mail server ... to ensure that ... e-mail adheres to the policies that are specified for a given site. The Agent intercepts e-mail normally bound for the mail server and checks to make sure that it conforms with policies .... If the e-mail adheres to the*

<u>policies ..., it is forwarded to the mail server</u> where it is routed to the intended recipient." (col. 3, ln. 27-36, emphasis added).

Consider claim 1 (sending), it has <u>no</u> step sending the secure e-mail to the security server. The e-mail is composed by the sender (step a), key procurement ensues with the security server (steps b-c), the e-mail is encrypted to form the secure e-mail (step d), and the secure e-mail is sent to the recipients. The encryption in step d is elsewhere than at the security server. This is now explicitly at the sender in the amended claim (and was implicitly elsewhere than at the security server even before, since it would be nonsensical for it to carry out password procurement with itself (steps b-c)).

Consider claim 11 (receiving), it also has <u>no</u> step sending the secure e-mail to the security server. Again, there is only key procurement with the security server (steps b-c). Step a of claim 11 is explicitly at the receiver. Step b is now also explicitly at the receiver in the amended claim (and was implicitly elsewhere than at the security server even before, since it would be nonsensical here as well for it to carry out password procurement with itself (steps b-c)).

If a secure e-mail were sent to a security server, as part of sending or receiving, and the security server were to do something with that secure e-mail, the result would not be "said secure e-mail" but rather a second, altered e-mail. This applies to all of claims 1, 11 and 20, and thus to all of the claims presently in the application.

In summary, McArdle and Hussey fail to teach or reasonably suggest a system that can implement secure email communication without intercepting each e-mail. This is a major disadvantage that the present claimed invention overcomes. As regards the rest of item 3, we urge that the dependant claims are allowable for the same reasons already discussed for independent parent claims 1, 11, and 21.

<u>CONCLUSION</u>

Applicant has endeavored to put this case into complete condition for allowance. It is thought that the §103 rejections have been completely rebutted. Applicant therefore asks that all objections and rejections now be withdrawn and that allowance of all claims presently in the case be granted.

Respectfully Submitted,

Raymond E. Roberts
Reg. No.: 38,597

Intellectual Property Law Offices
1901 S. Bascom Ave., Suite 660
Campbell, CA 95008

Telephone: 408.558.9950
Facsimile: 408.558.9960
E-mail: RRoberts@iplo.com

Customer No. 32112

32112
PATENT TRADEMARK OFFICE

Amendments to the claims

B1

1. (Currently amended): A method for sending a secure e-mail, comprising the steps of:

(a) composing an e-mail message by a sender, wherein said e-mail message includes a body field and at least one receiver field containing at least one receiver id representing at least one intended receiver;

(b) providing from said sender a sender id, a sender password, and all said receiver ids to a security server;

(c) receiving at said sender a message key and a message id which is unique for said e-mail message from said security server;

(d) encrypting said body field of said e-mail message based on said message key and enclosing said message id therewith to form the secure e-mail at said sender;

(e) mailing said secure e-mail ~~in conventional manner~~ to said receivers, wherein said secure e-mail itself is not communicated to or via said security server; and

(f) storing said message id, said message key, and all said receiver ids at said security server, to allow said security server to provide said message key to said receivers so that they may decrypt ~~and read~~ the secure e-mail.

2. (Original): The method of claim 1, wherein:

in said step (a) said e-mail message further includes a subject field; and

said step (d) includes encrypting said subject field.

3. (Original): The method of claim 1, wherein said sender id is associated with an e-mail address for said sender.

4. (Original): The method of claim 1, wherein said sender password is derived from a private password provided by said sender, to permit said sender to maintain said private password as private.

5. (Original): The method of claim 1, wherein said sender password has been previously stored for said sender.

6. (Original): The method of claim 1, further comprising authenticating said sender based on said sender id and said sender password after said step (b) and prior to proceeding with said step (c).

7. (Original): The method of claim 1, wherein said step (d) encrypts using a symmetric key encryption algorithm.

B1 cont

8. (Previously amended): The method of claim 1, wherein:

said step (e) includes mailing to at least one said receiver which is in a receiver list; and the method further comprising:

resolving said receiver list into a plurality of said receiver ids for said security server, to allow said security server to provide said message key to instances of said receivers which are members of said receiver list.

9. (Original): The method of claim 1, further comprising:

said step (b) includes providing a message hash based on said e-mail message to said security server; and

said step (c) includes receiving a first message seal from said security server based on said message hash; and

said step (d) includes enclosing the first message seal with the secure e-mail, to permit said security server comparing said first message seal with a second message seal taken from the secure e-mail as received to determine whether the secure e-mail has been altered while in transit to said receiver.

10. (Previously amended): The method of claim 1, wherein at least one of said steps (b) and (c) employs secure socket layer protocol in communications with said security server.

11. (Currently amended): A method for receiving a secure e-mail, comprising the steps of:

(a) accepting the secure e-mail by a receiver, wherein the secure e-mail includes a body field that is encrypted and a message id that uniquely identifies the secure e-mail;

(b) providing said message id as well as a receiver id and a receiver password for said receiver <u>from said receiver</u> to a security server;

(c) receiving a message key from said security server <u>at said receiver</u>; and

(d) decrypting the secure e-mail <u>at said receiver</u> based on said message key, to form an e-mail message which is readable~~ by said receiver~~.

B1 con't

12. (Original): The method of claim 11, wherein:

in said step (a) said secure e-mail further includes a subject field that is also encrypted; and

said step (d) includes decrypting said subject field.

13. (Original): The method of claim 11, wherein said receiver id is associated with an e-mail address for said receiver.

14. (Original): The method of claim 11, wherein said receiver password is derived from a private password provided by said receiver, to permit said receiver to maintain said private password as private.

15. (Original): The method of claim 11, wherein said receiver password has been previously stored for said receiver.

16. (Original): The method of claim 11, further comprising authenticating said receiver based on said receiver id and said receiver password after said step (b) and prior to proceeding with said step (c).

17. (Original): The method of claim 11, wherein said step (d) decrypts using a symmetric key decryption algorithm.

In accordance with the pre-OG notice dated January 31, 2003, Applicant has employed the "Manner of Making Amendments" encouraged therein

Amendments to the claims

18. (Previously amended) The method of claim 11, wherein:

the secure e-mail is sent by a sender and a first message seal based on the secure e-mail before it left control of said sender is stored by said security server;

said step (b) further includes also providing to said security server a second message seal which is taken from the secure e-mail as received by said receiver; and

said step (c) includes receiving an indication from said security server whether said first message seal and said second message seal match, to determine whether the secure e-mail was altered in transit.

B1 Amt

19. (Original): The method of claim 11, wherein at least one of said steps (b) and (c) employs secure socket layer protocol in communications with said security service.

20. (Currently amended): A system for communicating an e-mail message securely between a sender and a receiver, the system comprising:

a sending unit that composes the e-mail message for the sender, wherein the e-mail message includes a body field and a receiver field containing a receiver id representing the receiver;

said sending unit including a logic that provides a sender id, a sender password, and said receiver id to a security server;

said security server including a logic that replies to said sending unit with a message id, which is unique for the e-mail message, and a message key;

said security server further including a logic that stores said message id, said message key, and said receiver id;

said sending unit further including a logic that encrypts the e-mail message based on said message key and encloses said message id therewith to form a secure e-mail;

said sending unit yet further including a logic that e-mails said secure e-mail ~~in conventional manner~~ to the receiver, wherein said secure e-mail itself is not communicated to or via said security server;

a receiving unit that accepts said secure e-mail;

Amendments to the claims

B1
Con't

said receiving unit including a logic that provides said message id, said receiver id and a receiver password to said security server;

said security server yet further including a logic that replies to said receiving unit with said message key for said secure e-mail; and

said security server still further including a logic that decrypts said secure e-mail based on said message key into the e-mail message such that it is readable by the receiver.